That Pesky CFIDE Directory

Posted At : May 9, 2013 2:59 PM | Posted By : Mark Kruger
Related Categories: Coldfusion Security

If you are CF community connected (and if not why not?) you know about the latest "sub-zero" exploit to ColdFusion that once again targets the Administrator or adminapi directory under the CFIDE directory. It leverages tags that work with files from within these directories to place code on your server which can then be leveraged to do other things. Basically it can function as a hostile takeover of your server. See this entry titled **0-Day Exploit for ColdFusion** by the awesome folks at Edge web hosting for more information. It will point you to the Adobe Docs. The exploit targets CF 9 and 8 if I'm reading the source correctly.

The lockdown guide will give you a few *dozen* steps some of which will have you pulling out your hair unless you have carefully built your server. But the main "fix" for this exploit is fairly simple. Do *not allow arbitrary access to the CFIDE/Administrator and CFIDE/adminapi folders from the web*. This seems to be pretty head scratchingly obvious but you'd be surprised how many folks say *"But don't you need a password to get into the administrator?"*. Yes, and you need a key to get into your house too, but an "exploit" is rather like a brick through the window. To really secure your house you need a security system, good locks, good lighting, and a Rottweiler the size of a pony.

Why is it there in the first place?

This is a question I get sometimes. "I don't remember adding that virtual directory. How did it get there?" No you did not fugue off while adding web sites - unless you see one for a Ukrainian tether ball team or something - then probably yes you did fugue off. The real story is that when you install ColdFusion using selecting the "configure all websites" option during the install the CFIDE is mapped on all the sites on your web server as a physical (for the default site) or virtual (for everything else) directory. That's how it seems to "show up" everywhere. In addition the "connector" scripts - the ones you run to "remove all" and "add all" will add it as well. If you are like me you configure each site separately outside of the CF ecosystem. Then you join it to the ColdFusion engine using wsconfig. My servers use the multi-server config and I use the built in web-server (at ports 830X) to admin them from inside the network. When a new site is needed I add it in IIS or apache, then I use wsconfig to connect it to the ColdFusion instance I want. Yes it's extra steps and yes it requires more knowledge, but it's the way I like it. And I'm worth it. Doing it this way does not add the CFIDE directory by default - which is why if I need the scripts directory I use an alias or virtual and alter the setting within the admin.

But what I notice from time to time is that there *actually is* a CFIDE directory that shows up on some of my sites. How can this be? I've been so careful. Here's what happens. A team member - a developer - is assigned to a site for the first time. Perhaps this is the first site they have set up on their local environment, or perhaps they are sys admin challenged and don't know how to create an alias or virtual directory. For whatever reason the CFIDE physical directory is installed and is living in the root directory of the site. Then at some point the developer remembers (through the prodding of his project manager) that he needs to do regular updates of our subversion repository as a part of his task list. Suddenly (with apologies to Emeril if he's still alive and has not exploded) *BAM!* the CFIDE directory itself is now part of the source code. Our Jenkins CI server ignores this directory and does not deploy it to either staging or production but usually the initial site setup is not done by Jenkins. So one thing leads to another and the directory is deployed to staging (small yikes) or production (big yikes and a shudder).

Of course this is bad in more than one way. For one thing this directory has the vulnerabilities in question in the form of CF Scripts. For another it is likely *not* being used to admin the server - which means that updates in the form of hot fixes and security patches will never make it into this code. It might also end up being the *wrong version* of admin as the site code is transitioned from version to version. I'm not sure if that last is bad or good - but it is another thing to worry about.

In conclusion get out there and secure those directories (and other things). Let's make sure we are on top of this before it get's out of hand. :)